FPKIPA

Federal Public Key Infrastructure Policy Authority

X.509 Certificate and CRL Extensions Profile for the Shared Service Providers (SSP) Program. Change Proposal Number: 2015-02

To: Federal PKI Policy Authority (FPKIPA)

From: PKI Certificate Policy Working Group (CPWG)

Subject: Proposed modifications to the X.509 Certificate and CRL Extensions Profile for the Shared Service Providers (SSP) Program.

Date: April 2, 2015

Title: Modifying EKU Requirements

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate and CRL Extensions Profile for the Shared Service Providers (SSP) Program; dated January 7, 2008

Change Advocate's Contact Information:

Organization requesting change:

Change summary: Implementation of this request will give organizations a choice with respect to the use of the *anyExtendedKeyUsage* value.

Background:

In 2011 it was discovered that the Microsoft approach to identifying and validating code signing certificates created the potential for an otherwise valid end-user signing or authentication certificate to be exploited for use as a code signing certificate. Subsequently, a key management certificate successfully signed a macro in Microsoft EXCEL. This risk exists for the U.S. Federal PKI and other similarly operated PKIs where the code-signing attribute is asserted for the root certificate in the Microsoft trusted certificate store and the X.509 certificate extension "Extended Key Usage (EKU)" is either not present or includes the *anyExtendedKeyUsage* value. While this risk, can be mitigated by requesting that Microsoft remove the code-signing attribute from the Common Policy Root, some certificate issuers wish to be able to not include the a*nyExtendedKeyUsage* value in end user certificates. To allow this, the Federal PKI certificate profiles that require the use of the *anyExtendedKeyUsage* value must be modified.

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

Worksheet 5: End Entity Signature Certificate Profile

extKeyUsage	BOOLEAN		~~This extension need not appear. If included in a certificate that is specifically designated for use in a single application (e.g., code signing or signing content on PIV cards), the extension may be marked either critical or non-critical. If included in any other certificate (to support specific applications), the extension must may include the anyExtendedKeyUsage value and must should be marked non-critical. Additional key purposes may be specified.~~ This extension need not appear. If included the extension must be marked non-critical and may include the anyExtendedKeyUsage value. If anyExtendedKeyUsage is not included, in a PIV digital signature certificate the following 3 values for keyPurposeID must be included: id-kp-emailProtection; MSFT Document Signing; and Adobe Certified Document Signing. Additional key purposes may be specified. Note: Organizations that choose not to include the *anyExtendedKeyUsage* value may experience interoperability issues if the specific EKU required by an application is absent.
keyPurposeID		1.3.6.1.5.5.7.3.4	id-kp-emailProtection .
		1.3.6.1.4.1.311.10.3.12	MSFT Document Signing
		1.2.840.113583.1.1.5	Adobe Certified Document Signing
		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.

Worksheet 7: Certificate Profile for Computing and Communications Devices

extKeyUsage	BOOLEAN		This extension may be included as either a critical or non-critical extension if its inclusion is required by the application(s) for which the certificate will be used. ~~If the inclusion of this extension is not intended to limit acceptable uses of the subject public key, then the extension should be marked non-critical and the anyExtendedKeyUsage value should be included.~~ Additional key purposes may be specified
keyPurposeID		2.16.840.1.101.3.6.7	The id-PIV-content-signing keyPurposeID specifies that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics.

		~~2.5.29.37.0~~	~~anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.~~

Worksheet 9: PIV Authentication Certificate Profile

extKeyUsage	FALSE		This extension need not appear. If included to support specific applications, the extension ~~MUST~~ may include the anyExtendedKeyUsage value. If anyExtendedKeyUsage is not included, the following 3 values for keyPurposeID must be included Microsoft Smart Card Llogon, TLS Client Authentication and id-pkinit-KPClientAuth. Additional key purposes may be specified. Note: Organizations that choose not to include the anyExtendedKeyUsage value may experience interoperability issues if the specific EKU required by an application is absent.
keyPurposeID		1.3.6.1.4.1.311.20.2.2	Microsoft Smart Card Logon
		1.3.6.1.5.5.7.3.2	TLS client authentication
		1.3.6.1.5.2.3.4	id-pkinit-KPClientAuth
		1.3.6.1.5.5.7.3.21	id-kp-secureShellClient This key purpose value may be implemented as needed by the Subscriber
		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.

Estimated Cost: Changes to end entity certificates as a result of this Change Proposal are optional. Cost to implement is determined by the Entity choosing to implement the option. If issuers choose to restrict the uses of their certificates by including extended key usage extensions without *anyExtendedKeyUsage*, then some relying party applications may be unable to accept these certificates. Relying parties may incur costs associated with updating applications or issuing organizations may incur costs associated with reissuing certificates with the necessary key purposes.

Implementation Date:

The ability to make this change will be effective upon approval by the FPKIPA and incorporation into SSP Profiles. Implementation of the option should be coordinated between the CA and its customers.

Per the 10 March 2015 FPKIPA meeting, the FPKIPA will monitor the impact of this profile change and revisit this decision after gaining experience with the change to determine if the interoperability problems arise.

Prerequisites for Adoption:

Not Applicable.

Plan to Meet Prerequisites:

Not Applicable

Approval and Coordination Dates:

Date presented to CPWG:	January 14, 2015
Date presented to FPKIPA:	April 7, 2015
Date of approval by FPKIPA:	May 1, 2015